**信息安全工程师每日一练试题（2017/1/1）**

试题**1**： SQL 杀手蠕虫病毒发作的特征是什么()  
A、大量消耗网络带宽B、攻击个人PC终端C、破坏PC游戏程序D、攻击手机网络  
  
试题**2**： 信息网络安全的第一个时代()  
A、九十年代中叶B、九十年代中叶前C、世纪之交D、专网时代  
  
试题**3**： 网络管理中故障管理通常包括()  
A、监视、响应、诊断管理B、性能、分析、诊断管理C、监视、分析、资源管理  
  
试题**4**： 以下关于灾难恢复和数据备份的理解，说法正确的是：（）  
A．增量备份是备份从上次完全备份后更新的全部数据文件  
B．依据具备的灾难恢复资源程度的不同，灾难恢复能力分为7 个等级  
C．数据备份按数据类型划分可以划分为系统数据备份和用户数据备份  
D．如果系统在一段时间内没有出现问题，就可以不用再进行容灾演练了

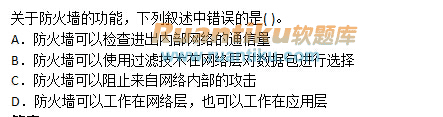
试题**5**： 以下对企业信息安全活动的组织描述不正确的是（）  
A. 企业应该在组织内建立发起和控制信息安全实施的管理框架。  
B.    企业应该维护被外部合作伙伴或者客户访问和使用的企业信息处理设施和信息资产的安全。  
C.在没有采取必要控制措施，包括签署相关协议之前，不应该授权给外部伙伴访问。应该让外部伙伴意识到其责任和必须遵守的规定。  
D.  企业在开展业务活动的过程中，应该完全相信员工，不应该对内部员工采取安全管控措施

试题**6**： 对于青少年而言，日常上网过程中，下列选项，存在安全风险的行为是?（）  
A、 将电脑开机密码设置成复杂的15位强密码B、 安装盗版的操作系统  
C、 在QQ聊天过程中不点击任何不明链接D、 避免在不同网站使用相同的用户名和口令

试题**7**： SSE-CMM工程过程区域中的风险过程包含哪些过程区域：（）  
A．评估威胁、评估脆弱性、评估影响B．评估威胁、评估脆弱性、评估安全风险  
C．评估威胁、评估脆弱性、评估影响、评估安全风险D．评估威胁、评估脆弱性、评估影响、验证和证实安全

试题**8**： 在信息安全管理体系中，带有高层目标的信息安全策略是被描述在（）  
A、信息安全管理手册B、信息安全管理制度C、信息安全指南和手册D、信息安全记录文档

试题**9**： 关于源代码审核，下列说法正确的是：（）  
A．人工审核源代码审校的效率低，但采用多人并行分析可以完全弥补这个缺点  
B．源代码审核通过提供非预期的输入并监视异常结果来发现软件故障，从而定位可能导致安全弱点的薄弱之处  
C．使用工具进行源代码审核，速度快，准确率高，已经取代了传统的人工审核  
D．源代码审核是对源代码检查分析，检测并报告源代码中可能导致安全弱点的薄弱之处

试题**10**： 

**信息安全工程师每日一练试题（2017/1/2）**

试题**1**： 在云计算虚拟化应用中，VXLAN技术处于OS工网络模型中2-3层间，它综合了2层交换的简单性与3层路由的跨域连接性。它是通过在UDP/IP上封装Mac地址而实现这一点的。在简单应用场合，vxLAN可以让虚拟机在数据中心之间的迁移变得更为简单。该技术是哪个公司主推的技术?()  
A、惠普 B、Juniper C、Cisco与Vmware D、博科Brocade  
  
试题**2**： D级为TCSEC的计算机安全等级中的最低级别()  
A、对B、错  
  
试题**3**： 依据我国相关的密码管理法规规定对研制加密算法、开发加密产品、销售加密产品单位，都要由有关主管部门指定或认定()  
A、是B、否  
  
试题**4**： 某电子商务网站在开发设计时，使用了威胁建模方法来分析电子商务网站所面临的威胁。STRIDE 是微软SDL 中提出的威胁建模方法，将威胁分为六类，为每一类威胁提供了标准的消减措施，Spoofing 是STRIDE 中欺骗类的威胁，以下威胁中哪个可以归入此类威胁？（）  
A.网站竞争对手可能雇佣攻击者实施DDos 攻击，降低网站访问速度  
B.网站使用http 协议进行浏览等操作，未对数据进行加密，可能导致用户传输信息泄漏，例如购买的商品金额等  
C.网站使用http 协议进行浏览等操作，无法确认数据与用户发出的是否一致，可能数据被中途篡改  
D.网站使用用户名、密码进行登录验证，攻击者可能会利用弱口令或其他方式获得用户密码，以该用户身份登录修改用户订单等信息  
  
试题**5**： 信息资产面临的主要威胁来源主要包括（）  
A.自然灾害B.系统故障C.内部人员操作失误D.以上都包括

试题**6**： 以下哪一个是对于参观者访问数据中心的最有效的控制？（）  
A.陪同参观者B.参观者佩戴证件C.参观者签字D.参观者由工作人员抽样检查  
  
试题**7**： 在设计某公司技术性的恢复策略时,以下哪个方面是安全人员最为关注的?（）  
A.目标恢复时间RTO B.业务影响分析C.从严重灾难中恢复的能力D.目标恢复点RPO  
  
试题**8**： 网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息不外泄的前提下，完成网络间数据的安全交换，下列隔离技术中，安全性最好的是？（）    
A、多重安全网关B、防火墙C、VLAN隔离D、物理隔离  
  
试题**9**： 时间戳的引入主要是为了防止：（）  
A．死锁B．丢失C．重放D．拥塞  
  
试题**10**： 以下哪一项不是工作在网络第二层的隧道协议？（）  
A、WTP B、l2F C、pptp D、L2TP

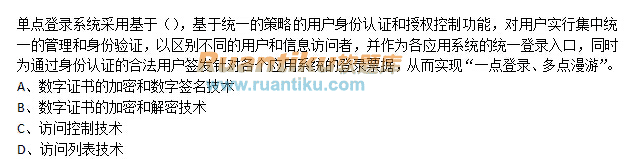
**信息安全工程师每日一练试题（2017/1/3）**

试题**1**： 某银行为用户提供网上服务，允许用户通过浏览器管理自己的银行账户信息。为保障通信的安全性，该 Web 服务器可选的协议是  （ ）  。  
A、POP B、SNMP C、HTTP D、HTTPS

试题**2**： 目前主流防火墙通常包括NAT模块、集中访问控制模块、临时访问端口表、认证与访问控制系统等() A、是B、否  
试题**3**： 以下哪些是可能存在的威胁因素？（）  
A.   设备老化故障B.病毒和蠕虫C. 系统设计缺陷D. 保安工作不得力

试题**4**： 以下哪一个不是网络隐藏技术？（）  
A.端口复用B."无端口技术"C.反弹端口技术D.DLL注入  
  
试题**5**： 关于信息保障技术框架（IATF），下列哪种说法是错误的？（）  
A、IATF强调深度防御，关注本地计算环境、区域边界、网络和基础设施、支撑性基础设施等多个领域的安全保障  
B、IATF强调深度防御，即对信息系统采用多层防护，实现组织的业务安全运作  
C、IATF强调从技术、管理和人等多个角度来保障信息系统的安全  
D、IATF强调的是以安全检测、漏洞监测和自适应填充“安全间隙”为循环来提高网络安全

试题**6**： 为了实现数据库的完整性控制，数据库管理员应向DBMS提出一组完整性规则来检查数据库中的数据，完整性规则主要由三部分组成，以下哪一个不是完整性规则的内容？（）  
A．完整性约束条件B．完整性检查机制C．完整性修复机制D．违约处理机制

试题**7**： 监听网络流量获取密码，之后使用这个密码试图完成未经授权访问的攻击方式被称为：（）  
A.穷举攻击B.字典攻击C.社会工程攻击D.重放攻击  
  
试题**8**： IPSEC密钥协商方式有：（）  
A、一种，手工方式B、两种，手工方式，IKE自动协商  
C、一种，IKE自动协商D、两种，IKE自动协商，隧道协商  
  
试题**9**：    
  
试题**10**： 扫描技术（）  
A、只能作为攻击工具B、只能作为防御工具

C、只能作为检查系统漏洞的工具D、既可以作为工具，也可以作为防御工具

**信息安全工程师每日一练试题（2017/1/4）**

试题**1**： 基于网络的入侵检测系统的输入信息源是（）。   
A、系统的审计日志             B、系统的行为数据 C、应用程序的事务日志文件     D、网络中的数据包   
  
试题**2**： 以下关于VPN说法正确的是（）。  
A、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路      
B、VPN指的是用户通过公用网络建立的临时的、逻辑隔离的、安全的连接      
C、VPN不能做到信息认证和身份认证      
D、VPN只能提供身份认证、不能提供加密数据的功能  
  
试题**3**： 最早研究计算机网络的目的是什么？()  
A、直接的个人通信；B、共享硬盘空间、打印机等设备；  
C、共享计算资源；D、大量的数据交换。  
试题**4**： DMZ 为非军事区()A、是B、否  
  
试题**5**： 网络监控的主动性表现为()  
A、及时发现、报警、勘察、处置B、及时查找、记录、分析、处理C、及时发现、记录、报警、处理  
  
试题**6**： 我国规定商用密码产品的研发、制造、销售和使用采取专控管理，必须经过审批，所依据的是()  
A、商用密码管理条例B、中华人民共和国计算机信息系统安全保护条例  
C、计算机信息系统国际联网保密管理规定D、中华人民共和国保密法  
  
试题**7**： 在提供给一个外部代理商访问信息处理设施前，一个组织应该怎么做？（）  
A.外部代理商的处理应该接受一个来自独立代理进行的IS 审计。  
B.外部代理商的员工必须接受该组织的安全程序的培训。  
C. 来自外部代理商的任何访问必须限制在停火区（DMZ）  
D.该组织应该进行风险评估，并制定和实施适当的控制。

试题**8**： 在安全人员的帮助下，对数据提供访问权的责任在于：（）  
A.   数据所有者.B.程序员C. 系统分析师.D. 库管员

试题**9**： 在逻辑访问控制中如果用户账户被共享，这种局面可能造成的最大风险是:（）  
A.非授权用户可以使用ID擅自进入.B.用户访问管理费时.C.很容易猜测密码.D.无法确定用户责任  
  
试题**10**： 下列岗位哪个在招聘前最需要进行背景调查？（）  
A.采购人员B.销售人员C.财务总监D.行政人员  
  
试题**11**： 建立应急响应计划最重要的是（）  
A.业务影响分析B.测试及演练C.各部门的参与D.管理层的支持  
  
试题**12**： 以下哪一个选项是从软件自身功能出发，进行威胁分析（）  
A.攻击面分析B.威胁建模C.架构设计D.详细设计

试题**13**： 《关于信息安全等级保护的实施意见》中信息和信息系统安全保护等级的第三级的定义是（）  
A.自主保护级B.指导保护级C.强制保护级D.监督保护级  
  
试题**14**： 对于Linux审计说法错误的是？（）  
A.Linux系统支持细粒度的审计操作  
B.Linux系统可以使用自带的软件发送审计日志到SOC平台  
C.Linux系统一般使用auditd进程产生日志文件  
D.Linux在secure日志中登陆成功日志和审计日志是一个文件  
  
试题**15**： 2016年国家网络安全宣传周主题是()  
A、 网络安全为人民，网络安全靠人民B、 共建网络安全，共享网络文明  
C、 网络安全同担，网络生活共享D、 我身边的网络安全  
  
试题**16**： 我们常提到的"在Windows操作系统中安装VMware，运行Linux虚拟机"属于( )。  
A、 存储虚拟化B、 内存虚拟化C、 系统虚拟化D、 网络虚拟化  
  
试题**17**： 以下哪一项是和电子邮件系统无关的？（）  
A.PEM(Privacyenhancedmail) B.PGP(PrettygoodPrivacy) C.X.500 D.X.400  
  
试题**18**： 数字签名是使用（）。  
A、己方的私钥B、己方的公钥C、对方的私钥D、对方的公钥

试题**19**： 下列SQL语句给出关系型数据库中的哪一类完整性约束条件?CREATETABLEStudent(idCHAR(8).SnameCHAR(20)NOTNULL，SageSMALLINT.PRIMARYKEY(id)（）  
A.实体完整性B.二维表完整性C.参照完整性D.自定义完整性

试题**20**： 2005 年4 月1日正式施行的《电子签名法》，被称为“中国首部真正意义上的信息化法律”，自此电子签名与传统手写签名和盖章具有同等的法律效力。以下关于电子签名说法错误的是：（）  
A．电子签名——是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据  
B．电子签名适用于民事活动中的合同或者其他文件、单证等文书  
C．电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务  
D．电子签名制作数据用于电子签名时，属于电子签名人和电子认证服务提供者共有

**信息安全工程师每日一练试题（2017/1/5）**

试题**1**： 甲向乙发送其数据签名，要验证该签名，乙可使用（ ）对该签名进行解密。  
A. 甲的私钥         B.甲的公钥         C. 乙的私钥               D. 乙的公钥  
  
试题**2**： 市场体系的重要组成部分是（ ）。   
A、信息市场B、金融市场C、劳动力市场D、房地产市场  
  
试题**3**： 电子签名(electronic signature)不能提供的安全性能是( )。  
A．电子文件的保密性B．电子文件的完整性C．鉴别文件签署者的身份D．文件签署者确认电子文件的内容   
  
试题**4**： 数字证书被撤销后存放于( )  
A. CA B.CRL C. ACL D.RA  
  
试题**5**： 下面哪个功能属于操作系统中的作业调度功能()  
A、控制用户的作业排序和运行B、对CPU,内存，外设以及各类程序和数据进行管理  
C、实现主机和外设的并行处理以及异常情况的处理D、处理输入/输出事务  
  
试题**6**： CDS的基本机构包括()  
A、内容监视中心、引擎、通讯三部分B、管理控制中心、数据分析器、通讯三部分

C、管理控制中心、引擎、通讯三部分  
  
试题**7**： 防火墙不具备（ ）动能。  
A.记录访问过程    B.查毒  C.包过滤    D.代理  
  
试题**8**： 假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（）。  
A.对称加密技术B.分组密码技术      C.公钥加密技术    D.单向函数密码技术

试题**9**： 一个组织的系统安全能力成熟度达到哪个级别以后，就可以对组织层面的过程进行规范的定义？   
A．2级——计划和跟踪B．3 级——充分定义C．4 级——量化控制D．5 级——持续改进

试题**10**： ISSE(信息系统安全工程)是美国发布的IATF3.0版本中提出的设计和实施信息系统（）。  
A．安全工程方法B．安全工程框架C．安全工程体系结构D．安全工程标准

**信息安全工程师每日一练试题（2017/1/6）**

试题**1**： 在实现信息安全的目标中，关于信息安全技术和管理之间的关系的说法不正确的是（ ）。  
A、产品和技术，要通过管理的组织职能才能发挥最好的作用  
B、技术不高但管理良好的系统远比技术高但管理混乱的系统安全  
C、信息安全技术可以解决所有信息安全问题  
D、实现信息安全是一个管理的过程，而并非仅仅是一个技术的过程

试题**2**： 以下关于入侵检测系统功能的叙述中，（）是不正确的。  
A、保护内部网络免受非法用户的侵入B、评估系统关键资源和数据文件的完整性  
C、识别已知的攻击行为D、统计分析异常行为  
  
试题**3**： Chinese Wall 模型的设计宗旨是：（）。  
A、用户只能访问哪些与已经拥有的信息不冲突的信息 B、用户可以访问所有信息  
C、用户可以访问所有已经选择的信息 D、用户不可以访问哪些没有选择的信息  
  
试题**4**： 在日常工作和生活中，经常需要从互联网上下载文件，此时必须要关注下载内容的安全性，谨慎使用下载完成的文件，以避免造成不必要的损害。以下关于互联网下载、使用等行为的说法，错误的是：（       ）

A．不随意下载使用来路不明的文件或程序

B．应进入软件的官方下载主页，或那些规模大、知名的网站进行下载

C．后缀名为 \*.exe、\*.rar、\*.zip、\*.doc等文件，下载后一定要先杀毒

D．在浏览网页过程中弹出的插件，都可以直接安装

试题**5**： 基于主机的入侵检测的主要作用是实时监视可疑的连接、系统日志检查，非法访问的闯入等()  
A、是B、否  
  
试题**6**： 隐患扫描（Scanner）和信息安全风险评估之间是怎样的关系？()  
A、隐患扫描就是信息安全风险评估B、隐患扫描是信息安全风险评估中的一部分，是技术脆弱性评估  
C、信息安全风险评估就是隐患扫描D、信息安全风险评估是隐患扫描的一个部分  
  
试题**7**： 下面哪项是信息安全管理体系中CHECK（检查）中的工作内容？（）  
A.按照计划的时间间隔进行风险评估的评审B.实施所选择的控制措施  
C.采取合适的纠正和预防措施。从其它组织和组织自身的安全经验中吸取教训  
D.确保改进达到了预期目标  
  
试题**8**： 浏览网页时，弹出“最热门的视频聊天室”的页面，遇到这种情况，一般怎么办?（）  
A、 现在网络主播很流行，很多网站都有，可以点开看看B、 安装流行杀毒软件，然后再打开这个页面  
C、 访问完这个页面之后，全盘做病毒扫描D、 弹出的广告页面，风险太大，不应该去点击  
  
试题**9**：    
  
试题**10**： 数字水印技术通过在数字化的多媒体数据中嵌入隐蔽的水印标记，可以有效地对数字多媒体数据的版权保护等功能。以下各项工，不属于数字水印在数字版权保护必须满足的基本应用需求的是（）  
A、安全性B、隐蔽性C、鲁棒性D、可见性

**信息安全工程师每日一练试题（2017/1/7）**

试题**1**： 保护计算机网络设备免受环境事故的影响属于信息安全的( )。  
A.人员安全B.物理安全C.数据安全D.操作安全  
  
试题**2**： IIS6.0支持的身份验证安全机制有4种验证方法，  其中安全级别最高的验证方法是( )。  
A、匿名身份验证 B、集成Windows身份验证 C、基本身份验证 D、摘要式身份验证  
  
试题**3**： 在Oracle中，将当前系统所有角色都授予scott，除Payroll外，下列哪个是正确的？（）  
A、ALTER  DEFAULT  ROLLE  USER　　scott  ALL  EXCEPT  Payroll  
B、ALTER   USER  DEFAULT  ROLLE  ALL  EXCEPT  Payroll  
C、ALTER   DEFAULT   ROLLE  ALL  EXCEPT   USER  scott   
D、ALTER   USER   scott  DEFAULT   ROLLE  ALL  EXCEPT  Payroll  
  
试题**4**： 关于防火墙的功能，下列叙述中错误的是( )．。  
A．防火墙可以检查进出内部网络的通信量  
B．防火墙可以使用过滤技术在网络层对数据包进行选择  
C．防火墙可以阻止来自网络内部的攻击  
D．防火墙可以工作在网络层，也可以工作在应用层   
  
试题**5**： 黑色星期四是指：()  
A、1998年11月3日星期四B、1999年6月24日星期四C、2000年4月13日星期四  
  
试题**6**： 包过滤防火墙工作在（）层。  
A．链路层              B． 网络层          C．传输层          D．应用层  
  
试题**7**： 下列古典密码算法是单表代换的是（）。  
A.Caesar      B.Hill        C. Vigenere      D.栅栏式密码  
  
试题**8**： 计算机安全事故发生时，下列哪些人不被通知或者最后才被通知：（）  
A.系统管理员B.律师C.恢复协调员D.硬件和软件厂商

试题**9**： 以下对RADIUS协议说法正确的是：（）  
A、它是一种B/S结构的协议B、它是一项通用的认证计费协议  
C、它使用TCP通信D、它的基本组件包括认证、授权和加密

试题**10**： 以下人员中，谁负有决定信息分类级别的责任？（）  
A．用户B．数据所有者C．审计员D．安全员

**信息安全工程师每日一练试题（2017/1/8）**

试题**1**： 信息系统安全属性分为三个方面，以下选项不属于安全属性的是（ ） 。  
A、可用性 B、保密性 C、系统性 D、完整性

试题**2**： 数字签名的功能不包括 （ ） 。  
A、防止发送方和接收方的抵赖行为 B、发送方身份确认 C、接收方身份确认 D、保证数据的完整性  
  
试题**3**： 代理服务器防火墙主要使用代理技术来阻断内部网络和外部网络之间的通信，达到隐蔽内部网络的目的。以下关于代理服务器防火墙的叙述中，（）是不正确的。  
A．仅“可以信赖的”代理服务才允许通过B．由于已经设立代理，因此任何外部服务都可以访问  
C．允许内部主机使用代理服务器访问InternetD．不允许外部主机连接到内部安全网络  
试题**4**： 数据库的()是指如何组织、管理、保护和处理敏感信息的指导思想。它包括安全管理策略、访问控制策略和信息控制策略。  
A、安全策略B、管理策略C、控制策略D、访问策略   
  
试题**5**： 以下哪一项是信息资产自身存在的脆弱性的例子()  
A、漏洞B、网络、系统结构复杂C、不良习惯D、系统缺省配置E、以上各项都是  
  
试题**6**： 主要用于通信加密机制的协议是( )  
A、 HTTP B、 FTP C、 TELNET D、 SSL  
  
试题**7**： 操作系统中\_\_\_\_文件系统支持加密功能( )  
A、 NTFS B、 FAT32 C、 FAT D、 EFS  
  
试题**8**： 信息安全保障技术框架(InformationAssurance TechnicalFramework，IATF)由美国国家安全局(NSA)发布，最初目的是为保障美国政府和工业的信息基础设施安全提供技术指南，其中，提出需要防护的三类“焦点区域”是：（）  
A．网络和基础设施区域边界重要服务器B．网络和基础设施区域边界计算环境  
C．网络机房环境网络接口计算环境D．网络机房环境网络接口重要服务器

试题**9**：    
  
试题**10**： 

**2017/1/1 1~5 A B A A 无 6~10 B C B B C**

**2017/1/2 1~5 C A A D D 6~10 A B A C A**

**2017/1/3 1~5 D A B D D 6~10 C D B A D**

**2017/1/4 1~5 D B C A C 6~10 A D A D C**

**11~15 D A D D A 16~20 C C A A D**

**2017/1/5 1~5 B A A B A 6~10 C B A B A**

**2017/1/6 1~5 C A A D A 6~10 B A D A D**

**2017/1/7 1~5 B B D C A 6~10 B A B B B**

**2017/1/8 1~5 C C B A E 6~10 D A B C C**